

Scenario 1: Network Traffic Analysis

Task1.1: -

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|----------------|----------|--------|---|
| 1 | 10:00:00.000 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[69] |
| 6 | 10:00:06.003 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[70] |
| 8 | 13:58:47.998 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3107 Len=38 |
| 10 | 18:00:53.997 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3107 Len=38 |
| 12 | 20:00:56.767 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[71] |
| 13 | 20:00:59.569 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[72] |
| 17 | 35:53:22.19 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=18 |
| 18 | 35:53:30.560 | 192.168.69.1 | 192.168.69.255 | UDP | 62 | 68 Unconfirmed-REQ i-Am device,33000 |
| 29 | 35:53:66.04 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | I-Am-Router-To-Network |
| 21 | 35:53:93.85 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 - 47889 Len=26 |
| 22 | 35:54:39.25 | 192.168.69.1 | 192.168.69.255 | UDP | 72 | 47889 - 47889 Len=26 |
| 24 | 35:55:06.76 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3110 Len=26 |
| 25 | 35:55:07.013 | 192.168.69.1 | 192.168.69.255 | UDP | 66 | 47889 - 47889 Len=24 |
| 26 | 35:57:41.36 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 72 | 68 Unconfirmed-REQ i-Am device,33000 |
| 28 | 35:57:41.717 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=25 |
| 29 | 35:57:44.647 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=26 |
| 30 | 35:57:57.739 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 69 | I-Am-Router-To-Network |
| 32 | 36:39:51.51 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3110 Len=40 |
| 34 | 40:00:13.56 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[73] |
| 36 | 40:01:56.541 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3110 Len=26 |
| 38 | 45:44:27.28 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3110 Len=26 |
| 40 | 45:44:29.569 | 192.168.69.1 | 192.168.21.204 | UDP | 69 | 47889 - 3110 Len=26 |
| 42 | 59:00:16.97 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[74] |
| 44 | 59:00:46.381 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3110 Len=26 |
| 46 | 59:00:49.16 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3110 Len=38 |
| 48 | 59:09:27.923 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[75] |
| 50 | 70:00:13.29 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[76] |
| 54 | 80:00:10.45 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[77] |
| 56 | 80:00:10.56 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | 68 Unconfirmed-REQ readProperty[235] loop,1 present-value |
| 58 | 89:00:33.02 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[78] |
| 59 | 98:00:77.133 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 69 | Confirmed-REQ i-Am device,33000 |
| 64 | 98:00:93.37 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 - 47889 Len=18 |
| 65 | 98:00:97.19 | 192.168.69.1 | 192.168.69.255 | UDP | 62 | 47889 - 47889 Len=9 |
| 67 | 98:00:97.95 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,33000 |
| 68 | 98:00:98.42 | 192.168.69.1 | 192.168.69.255 | UDP | 72 | 47889 - 47889 Len=38 |
| 69 | 98:00:99.44 | 192.168.69.1 | 192.168.21.100 | UDP | 68 | 47889 - 47889 Len=26 |
| 70 | 98:02:76.43 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|--------------|----------------|----------|--------|--|
| 70 | 10:00:00.743 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 71 | 89:53:93.60 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=24 |
| 72 | 89:54:28.70 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 72 | 68 Unconfirmed-REQ i-Am device,33000 |
| 74 | 99:01:27.00 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=15 |
| 75 | 99:01:27.850 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=9 |
| 76 | 99:01:27.917 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 69 | I-Am-Router-To-Network |
| 78 | 99:01:27.919 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3111 Len=46 |
| 79 | 99:01:27.919 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[79] |
| 80 | 99:01:27.919 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | 68 Unconfirmed-REQ readPropertyMultiple[79] |
| 82 | 10:00:01.744 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 85 | 107:00:26.5 | 192.168.69.1 | 192.168.69.255 | UDP | 69 | 47889 - 47889 Len=24 |
| 86 | 107:00:26.503 | 192.168.69.1 | 192.168.69.255 | UDP | 62 | 47889 - 47889 Len=29 |
| 87 | 107:00:26.506 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,33000 |
| 88 | 107:00:26.509 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 - 47889 Len=26 |
| 90 | 107:00:26.511 | 192.168.69.1 | 192.168.69.255 | UDP | 72 | 47889 - 47889 Len=30 |
| 92 | 107:00:26.513 | 192.168.69.1 | 192.168.69.255 | BACnet.. | 66 | 47889 - 47889 Len=24 |
| 94 | 107:00:26.515 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 96 | 107:00:26.517 | 192.168.69.1 | 192.168.21.204 | UDP | 72 | 47889 - 3111 Len=38 |
| 98 | 108:40:56.64 | 192.168.69.1 | 192.168.21.204 | UDP | 143 | 47889 - 3111 Len=101 |
| 100 | 108:40:56.644 | 192.168.69.1 | 192.168.21.204 | UDP | 71 | 47889 - 3111 Len=29 |
| 102 | 108:40:56.645 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 - 3111 Len=46 |
| 104 | 108:40:56.645 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Confirmed-REQ readProperty[237] loop,1 present-value |
| 105 | 108:40:56.646 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 109 | 108:40:56.648 | 192.168.69.1 | 192.168.21.204 | UDP | 113 | 47889 - 3111 Len=71 |
| 112 | 109:11:22.58 | 192.168.69.1 | 192.168.21.204 | UDP | 91 | 47889 - 3111 Len=49 |
| 114 | 109:20:49.98 | 192.168.69.1 | 192.168.21.204 | UDP | 70 | 47889 - 3111 Len=28 |
| 116 | 109:39:86.64 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[80] |
| 119 | 112:7:79.507 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 120 | 112:7:83.00 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 123 | 112:11:24.289 | 192.168.69.1 | 192.168.21.204 | UDP | 69 | 47889 - 3111 Len=38 |
| 125 | 117:8:32.244 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 127 | 118:6:95.618 | 192.168.69.1 | 192.168.21.204 | UDP | 89 | 47889 - 3111 Len=38 |
| 128 | 118:8:72.447 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 69 | Confirmed-REQ readProperty[238] loop,1 present-value |
| 131 | 119:39:00.254 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[81] |
| 133 | 122:8:88.9188 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |

Task1.2: -

| ip.dst == 192.168.60.1 | | | | | |
|------------------------|------------|----------------|--------------|-----------|---|
| No. | Time | Source | Destination | Protocol | Length Info |
| 1 | 0.000000 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[69] |
| 5 | 9.998947 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[70] |
| 7 | 13.573216 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3107 → 47809 Len=17 |
| 9 | 18.623781 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3107 → 47809 Len=17 |
| 11 | 19.996931 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[71] |
| 13 | 29.995796 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[72] |
| 15 | 35.527173 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Unconfirmed-REQ who-Is |
| 16 | 35.530014 | 192.168.21.100 | 192.168.60.1 | BACnet... | 68 Unconfirmed-REQ i-Am device,35200 |
| 19 | 35.535427 | 192.168.21.100 | 192.168.60.1 | BACnet... | 72 Unconfirmed-REQ i-Am device,3535 |
| 23 | 35.553898 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 27 | 35.652383 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Who-Is-Router-To-Network |
| 31 | 36.356887 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3110 → 47809 Len=28 |
| 33 | 39.994064 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[73] |
| 35 | 40.660711 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 37 | 45.633899 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 39 | 45.864183 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 41 | 49.993316 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[74] |
| 43 | 50.646973 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 45 | 50.893068 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3110 → 47809 Len=17 |
| 47 | 59.991313 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[75] |
| 49 | 69.996142 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[76] |
| 53 | 79.988667 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[77] |
| 56 | 88.882514 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[235] loop,1 present-value |
| 57 | 89.987089 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[78] |
| 60 | 98.886793 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Unconfirmed-REQ who-Is |
| 61 | 98.882169 | 192.168.21.100 | 192.168.60.1 | BACnet... | 72 Unconfirmed-REQ i-Am device,3535 |
| 62 | 98.884767 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[236] loop,1 present-value |
| 63 | 98.887789 | 192.168.21.100 | 192.168.60.1 | BACnet... | 68 Unconfirmed-REQ i-Am device,35200 |
| 68 | 98.912331 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 73 | 99.613084 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Who-Is-Router-To-Network |
| 77 | 99.610989 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 79 | 99.985898 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[79] |
| 81 | 103.966877 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 83 | 107.687653 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Unconfirmed-REQ who-Is |
| 84 | 107.690962 | 192.168.21.100 | 192.168.60.1 | BACnet... | 68 Unconfirmed-REQ i-Am device,35200 |
| 89 | 107.713841 | 192.168.21.100 | 192.168.60.1 | BACnet... | 72 Unconfirmed-REQ i-Am device,3535 |
| 93 | 107.764235 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 95 | 107.963437 | 192.168.21.204 | 192.168.60.1 | UDP | 64 3111 → 47809 Len=22 |
| 97 | 108.363834 | 192.168.21.204 | 192.168.60.1 | UDP | 76 3111 → 47809 Len=34 |
| 99 | 108.664371 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 101 | 108.764480 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 103 | 108.864426 | 192.168.21.204 | 192.168.60.1 | UDP | 66 3111 → 47809 Len=24 |
| 105 | 108.876674 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[237] loop,1 present-value |
| 107 | 108.964756 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 108 | 108.983835 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 111 | 109.064899 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 113 | 109.165122 | 192.168.21.204 | 192.168.60.1 | UDP | 71 3111 → 47809 Len=29 |
| 115 | 109.984236 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[80] |
| 118 | 112.789308 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 120 | 113.620554 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 122 | 113.990958 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 124 | 117.828201 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 126 | 118.678445 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 129 | 118.875529 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[238] loop,1 present-value |
| 130 | 119.982989 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[81] |
| 132 | 122.873464 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |

| ip.dst == 192.168.60.1 | | | | | |
|------------------------|------------|----------------|--------------|-----------|---|
| No. | Time | Source | Destination | Protocol | Length Info |
| 73 | 99.013084 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Who-Is-Router-To-Network |
| 77 | 99.610989 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 79 | 99.985898 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[79] |
| 81 | 103.966877 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 83 | 107.687653 | 192.168.21.100 | 192.168.60.1 | BACnet... | 60 Unconfirmed-REQ who-Is |
| 84 | 107.690962 | 192.168.21.100 | 192.168.60.1 | BACnet... | 68 Unconfirmed-REQ i-Am device,35200 |
| 89 | 107.713841 | 192.168.21.100 | 192.168.60.1 | BACnet... | 72 Unconfirmed-REQ i-Am device,3535 |
| 93 | 107.764235 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 95 | 107.963437 | 192.168.21.204 | 192.168.60.1 | UDP | 64 3111 → 47809 Len=22 |
| 97 | 108.363834 | 192.168.21.204 | 192.168.60.1 | UDP | 76 3111 → 47809 Len=34 |
| 99 | 108.664371 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 101 | 108.764480 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 103 | 108.864426 | 192.168.21.204 | 192.168.60.1 | UDP | 66 3111 → 47809 Len=24 |
| 105 | 108.876674 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[237] loop,1 present-value |
| 107 | 108.964756 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 108 | 108.983835 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 111 | 109.064899 | 192.168.21.204 | 192.168.60.1 | UDP | 70 3111 → 47809 Len=28 |
| 113 | 109.165122 | 192.168.21.204 | 192.168.60.1 | UDP | 71 3111 → 47809 Len=29 |
| 115 | 109.984236 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[80] |
| 118 | 112.789308 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 120 | 113.620554 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 122 | 113.990958 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 124 | 117.828201 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 126 | 118.678445 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |
| 129 | 118.875529 | 192.168.21.100 | 192.168.60.1 | BACnet... | 65 Complex-ACK readProperty[238] loop,1 present-value |
| 130 | 119.982989 | 192.168.21.100 | 192.168.60.1 | BACnet... | 61 Confirmed-REQ readPropertyMultiple[81] |
| 132 | 122.873464 | 192.168.21.204 | 192.168.60.1 | UDP | 60 3111 → 47809 Len=17 |

Task1.3: -

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|---|
| 1 | 08:09:09 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[69] |
| 2 | 08:10:09 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[69] |
| 5 | 9.998947 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[70] |
| 6 | 10.008603 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[70] |
| 7 | 13.573216 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3107 .. 47889 Len=17 |
| 8 | 13.584798 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3187 Len=38 |
| 9 | 18.623781 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3107 .. 47889 Len=17 |
| 10 | 18.635907 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3187 Len=38 |
| 11 | 18.636001 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[71] |
| 12 | 20.659676 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[71] |
| 13 | 20.995796 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[72] |
| 14 | 30.003486 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[72] |
| 15 | 35.527173 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 68 | Unconfirmed-REQ who-is |
| 16 | 35.530914 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,35200 |
| 17 | 35.532219 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=18 |
| 18 | 35.535354 | 192.168.69.1 | 192.168.69.255 | UDP | 62 | 47889 .. 47889 Len=20 |
| 19 | 35.535427 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 72 | Unconfirmed-REQ i-Am device,3535 |
| 20 | 35.536604 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,33000 |
| 21 | 35.539385 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=26 |
| 22 | 35.542952 | 192.168.69.1 | 192.168.69.255 | UDP | 72 | 3110 .. 47889 Len=30 |
| 23 | 35.553698 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 24 | 35.559676 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3110 Len=26 |
| 25 | 35.560813 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=24 |
| 26 | 35.574136 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ i-Am device,33003 |
| 27 | 35.652383 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 68 | Who-Is-Router-To-Network |
| 28 | 35.655817 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=15 |
| 29 | 35.656467 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=9 |
| 30 | 35.657739 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | I-Am-Router-To-Network |
| 31 | 36.350887 | 192.168.21.204 | 192.168.69.1 | UDP | 70 | 3110 .. 47889 Len=28 |
| 32 | 36.395154 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3110 Len=46 |
| 33 | 39.90344 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[73] |
| 34 | 44.681356 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[73] |
| 35 | 46.690711 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 36 | 46.615641 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3110 Len=26 |
| 37 | 45.633899 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 38 | 45.642728 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3110 Len=26 |
| 39 | 45.864183 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 40 | 45.879459 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3110 Len=38 |

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|---|
| 39 | 45.864183 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 40 | 45.879459 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3110 Len=38 |
| 41 | 49.993316 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[74] |
| 42 | 50.001697 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[74] |
| 43 | 50.644973 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 44 | 50.653639 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3110 Len=38 |
| 45 | 50.693866 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3110 .. 47889 Len=17 |
| 46 | 50.904916 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3110 Len=26 |
| 47 | 59.991313 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[75] |
| 48 | 59.997923 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[75] |
| 49 | 69.990142 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[76] |
| 50 | 70.001329 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[76] |
| 53 | 79.988607 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[77] |
| 54 | 80.001845 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[77] |
| 55 | 80.002401 | 192.168.21.100 | 192.168.69.1 | UDP | 68 | 47889 .. 47889 Len=18 |
| 56 | 80.092514 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 65 | Complex-ACK readPropertyMultiple[230] loop,1 present-value |
| 57 | 80.987889 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[78] |
| 58 | 89.993325 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[78] |
| 59 | 98.877133 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Confirmed-REQ readProperty[230] loop,1 present-value |
| 60 | 98.880793 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 66 | Unconfirmed-REQ who-is |
| 61 | 98.882169 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 72 | Unconfirmed-REQ i-Am device,3535 |
| 62 | 98.884767 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 65 | Complex-ACK readProperty[230] loop,1 present-value |
| 63 | 98.887789 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,35200 |
| 64 | 98.891307 | 192.168.69.1 | 192.168.21.100 | UDP | 68 | 47889 .. 47889 Len=18 |
| 65 | 98.899710 | 192.168.69.1 | 192.168.69.255 | UDP | 62 | 47889 .. 47889 Len=20 |
| 66 | 98.903675 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,33000 |
| 67 | 98.908842 | 192.168.69.1 | 192.168.69.255 | UDP | 72 | 47889 .. 47889 Len=38 |
| 68 | 98.912331 | 192.168.21.204 | 192.168.69.1 | UDP | 68 | 3111 .. 47889 Len=17 |
| 69 | 98.915944 | 192.168.69.1 | 192.168.69.255 | UDP | 68 | 47889 .. 47889 Len=26 |
| 70 | 98.927643 | 192.168.69.1 | 192.168.21.204 | UDP | 68 | 47889 .. 3111 Len=26 |
| 71 | 98.939368 | 192.168.69.1 | 192.168.69.255 | UDP | 66 | 47889 .. 47889 Len=24 |
| 72 | 98.942876 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ i-Am device,33003 |
| 73 | 98.946884 | 192.168.21.100 | 192.168.69.1 | BACnet.. | 65 | Complex-ACK readProperty[230] loop,1 present-value |
| 74 | 99.017288 | 192.168.69.1 | 192.168.69.255 | UDP | 60 | 47889 .. 47889 Len=18 |
| 75 | 99.017859 | 192.168.69.1 | 192.168.69.255 | UDP | 60 | 47889 .. 47889 Len=9 |
| 76 | 99.019217 | 192.168.69.1 | 192.168.21.100 | BACnet.. | 66 | I-Am-Router-To-Network |
| 77 | 99.610989 | 192.168.21.204 | 192.168.69.1 | UDP | 70 | 3111 .. 47889 Len=28 |
| 78 | 99.691849 | 192.168.69.1 | 192.168.21.204 | UDP | 88 | 47889 .. 3111 Len=46 |

| ip.addr == 192.168.60.1 | | | | | | |
|-------------------------|----------------|----------------|----------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 77 99.618989 | 192.168.21.204 | 192.168.60.1 | 192.168.21.204 | UDP | 70 | 3111 - 47889 Len=28 |
| 78 99.691849 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 88 | 47889 - 3111 Len=46 |
| 79 99.985898 | 192.168.21.100 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[79] |
| 80 99.99.993469 | 192.168.60.1 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[79] |
| 81 107.696107 | 192.168.21.204 | 192.168.60.1 | 192.168.21.204 | UDP | 66 | 3111 - 47889 Len=17 |
| 82 103.374844 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 83 107.687653 | 192.168.21.100 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 69 | Unconfirmed-REQ who-Is |
| 84 107.690962 | 192.168.60.1 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 69 | Unconfirmed-REQ 1-Am device,35200 |
| 85 107.692265 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | UDP | 66 | 47889 - 47889 Len=18 |
| 86 107.696103 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | UDP | 62 | 47889 - 47889 Len=20 |
| 87 107.697250 | 192.168.60.1 | 192.168.21.100 | 192.168.21.100 | BACnet.. | 68 | Unconfirmed-REQ i-Am device,33000 |
| 88 107.706125 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | UDP | 68 | 47889 - 47889 Len=26 |
| 89 107.710141 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | BACnet.. | 68 | Confirmed-REQ i-Am device,33503 |
| 90 107.716913 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | UDP | 72 | 47889 - 47889 Len=24 |
| 91 107.730871 | 192.168.60.1 | 192.168.60.255 | 192.168.60.255 | UDP | 66 | 47889 - 47889 Len=24 |
| 92 107.732335 | 192.168.60.1 | 192.168.21.100 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ i-Am device,33003 |
| 93 107.764235 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 66 | 3111 - 47889 Len=17 |
| 94 107.774745 | 192.168.60.1 | 192.168.21.204 | 192.168.21.204 | UDP | 68 | 47889 - 3111 Len=26 |
| 95 107.963437 | 192.168.21.204 | 192.168.60.1 | 192.168.60.255 | UDP | 64 | 3111 - 47889 Len=22 |
| 96 108.592160 | 192.168.60.1 | 192.168.21.204 | 192.168.60.255 | UDP | 72 | 47889 - 3111 Len=36 |
| 97 108.363834 | 192.168.60.1 | 192.168.21.204 | 192.168.60.255 | UDP | 76 | 3111 - 47889 Len=34 |
| 98 108.405640 | 192.168.60.1 | 192.168.21.204 | 192.168.60.255 | UDP | 142 | 47889 - 3111 Len=101 |
| 99 108.664371 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 78 | 3111 - 47889 Len=28 |
| 100 108.705014 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 71 | 47889 - 3111 Len=29 |
| 101 108.764480 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 70 | 3111 - 47889 Len=28 |
| 102 108.797264 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 88 | 47889 - 3111 Len=46 |
| 103 108.864426 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 66 | 3111 - 47889 Len=24 |
| 104 108.900265 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | BACnet.. | 60 | Confirmed-REQ readProperty[237] loop,1 present-value |
| 105 108.976674 | 192.168.21.100 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 65 | Complex-ACK readProperty[237] loop,1 present-value |
| 106 108.888244 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 107 108.964756 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 78 | 3111 - 47889 Len=28 |
| 108 108.983835 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 66 | 3111 - 47889 Len=17 |
| 109 108.991473 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 110 109.019586 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 113 | 47889 - 3111 Len=71 |
| 111 109.090020 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 78 | 3111 - 47889 Len=28 |
| 112 109.112258 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 91 | 47889 - 3111 Len=49 |
| 113 109.166123 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 71 | 3111 - 47889 Len=29 |
| 114 109.204968 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 78 | 47889 - 3111 Len=28 |
| 115 109.984236 | 192.168.21.100 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[80] |
| 116 109.989646 | 192.168.60.1 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[80] |
| 118 112.789308 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 60 | 3111 - 47889 Len=17 |
| 119 112.796507 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 120 113.626554 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 60 | 3111 - 47889 Len=17 |
| 121 113.639160 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=38 |
| 122 113.996958 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 66 | 3111 - 47889 Len=17 |
| 123 114.006280 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 124 117.832801 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 60 | 3111 - 47889 Len=17 |
| 125 117.832244 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |
| 126 118.678445 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 60 | 3111 - 47889 Len=17 |
| 127 118.6956318 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 80 | 47889 - 3111 Len=38 |
| 128 118.872447 | 192.168.60.1 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Confirmed-REQ readProperty[238] loop,1 present-value |
| 129 118.875529 | 192.168.21.100 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 65 | Complex-ACK readProperty[238] loop,1 present-value |
| 130 119.982989 | 192.168.21.100 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[81] |
| 131 119.999254 | 192.168.60.1 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[81] |
| 132 122.873464 | 192.168.21.204 | 192.168.60.1 | 192.168.60.1 | UDP | 60 | 3111 - 47889 Len=17 |
| 133 122.889188 | 192.168.60.1 | 192.168.21.204 | 192.168.60.1 | UDP | 68 | 47889 - 3111 Len=26 |

Task1.4: -

| ip.addr == 192.168.60.1 && ip.addr == 192.168.21.1005 | | | | | | |
|---|------------|----------------|----------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 1 | 0.000000 | 192.168.60.1 | 192.168.60.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[69] |
| 2 | 0.010000 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[69] |
| 5 | 0.000047 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[70] |
| 6 | 0.000093 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[70] |
| 11 | 19.990333 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[71] |
| 12 | 20.000370 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[71] |
| 13 | 20.000370 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[72] |
| 14 | 30.003486 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[72] |
| 15 | 31.021173 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Unconfirmed-RDQ who-is |
| 16 | 31.530014 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,35200 |
| 19 | 31.535427 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 72 | Unconfirmed-REQ 1-Am device,3535 |
| 20 | 31.536004 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,30000 |
| 26 | 31.574130 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,30083 |
| 27 | 31.552363 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Who-Is-Router-To-Network |
| 30 | 31.657739 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | I-Am-Router-To-Network |
| 33 | 31.694064 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[73] |
| 34 | 41.001356 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[73] |
| 41 | 49.003318 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[74] |
| 42 | 50.001987 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[74] |
| 47 | 50.001313 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[75] |
| 48 | 50.007703 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[75] |
| 49 | 61.000142 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[76] |
| 50 | 70.001329 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[76] |
| 53 | 79.000607 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[77] |
| 54 | 80.001845 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[77] |
| 55 | 81.879849 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 56 | 81.882514 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 57 | 81.887009 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[78] |
| 58 | 81.887123 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[78] |
| 60 | 81.880793 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 61 | 81.882169 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 62 | 91.004707 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,35200 |
| 63 | 91.004707 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 64 | 91.004709 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,35200 |
| 66 | 91.005075 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ 1-Am device,35000 |
| 72 | 91.042878 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ 1-Am device,35000 |
| 73 | 91.013094 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Who-Is-Router-To-Network |
| 76 | 91.019217 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | I-Am-Router-To-Network |
| 79 | 91.005000 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[79] |
| 80 | 91.003469 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[79] |
| 83 | 107.687053 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Unconfirmed-REQ who-is |
| 84 | 107.690002 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 68 | Unconfirmed-REQ 1-Am device,35200 |
| 87 | 107.697250 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,35000 |
| 89 | 107.713041 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,35100 |
| 92 | 107.732339 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,35000 |
| 104 | 109.076572 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-REQ readProperty[238] loop_1 present-value |
| 105 | 109.076574 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 115 | 109.004206 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Confirmed-RDQ readPropertyMultiple[80] |
| 116 | 109.004206 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[80] |
| 129 | 110.872447 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 129 | 110.872529 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 130 | 110.882089 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 63 | Confirmed-RDQ readPropertyMultiple[81] |
| 131 | 110.996254 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[81] |

| ip.addr == 192.168.60.1 && ip.addr == 192.168.21.100 | | | | | | |
|--|------------|----------------|----------------|----------|--------|--|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 54 | 0.000045 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[73] |
| 55 | 0.000049 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 56 | 0.002514 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 57 | 0.000009 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-RDQ readPropertyMultiple[78] |
| 58 | 0.003235 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 61 | Complex-ACK readPropertyMultiple[78] |
| 59 | 0.00071233 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 60 | 0.00000703 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 61 | 0.00000703 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Unconfirmed-RDQ 1-Am device,35200 |
| 62 | 0.00000703 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 63 | 0.00000703 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,35000 |
| 64 | 0.00000705 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 72 | Unconfirmed-REQ 1-Am device,35000 |
| 72 | 0.00000705 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 72 | Unconfirmed-REQ 1-Am device,35000 |
| 73 | 0.00000705 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Who-Is-Router-To-Network |
| 76 | 0.00000705 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | I-Am-Router-To-Network |
| 79 | 0.00000705 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 61 | Confirmed-REQ readPropertyMultiple[79] |
| 80 | 0.00000705 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[79] |
| 83 | 107.687053 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Unconfirmed-REQ who-is |
| 84 | 107.690002 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 68 | Unconfirmed-REQ 1-Am device,35200 |
| 87 | 107.697250 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Unconfirmed-REQ 1-Am device,35000 |
| 89 | 107.713041 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,35100 |
| 92 | 107.732339 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 73 | Unconfirmed-REQ 1-Am device,35000 |
| 104 | 109.076572 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-REQ readProperty[238] loop_1 present-value |
| 105 | 109.076574 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 115 | 109.004206 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Confirmed-RDQ readPropertyMultiple[80] |
| 116 | 109.004206 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[80] |
| 129 | 110.872447 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 60 | Confirmed-RDQ readProperty[238] loop_1 present-value |
| 129 | 110.872529 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 60 | Complex-ACK readProperty[238] loop_1 present-value |
| 130 | 110.882089 | 192.168.21.100 | 192.168.60.1 | BACnet.. | 63 | Confirmed-RDQ readPropertyMultiple[81] |
| 131 | 110.996254 | 192.168.60.1 | 192.168.21.100 | BACnet.. | 67 | Complex-ACK readPropertyMultiple[81] |

Scenario 2- VoIP Security Analysis

Task 2.1: -

Common VoIP issues include:

1. Network Congestion: High network traffic leading to call quality degradation or drops.
2. Jitter and Latency: Inconsistent packet arrival times causing audio quality issues.
3. Packet Loss: Missing packets can result in call drops or poor audio quality.
4. Codec Mismatch: Incompatibility between codecs can lead to audio issues.

Identified Issue in this Scenario:

Frequent call drops suggest potential issues with network congestion, packet loss, or jitter.

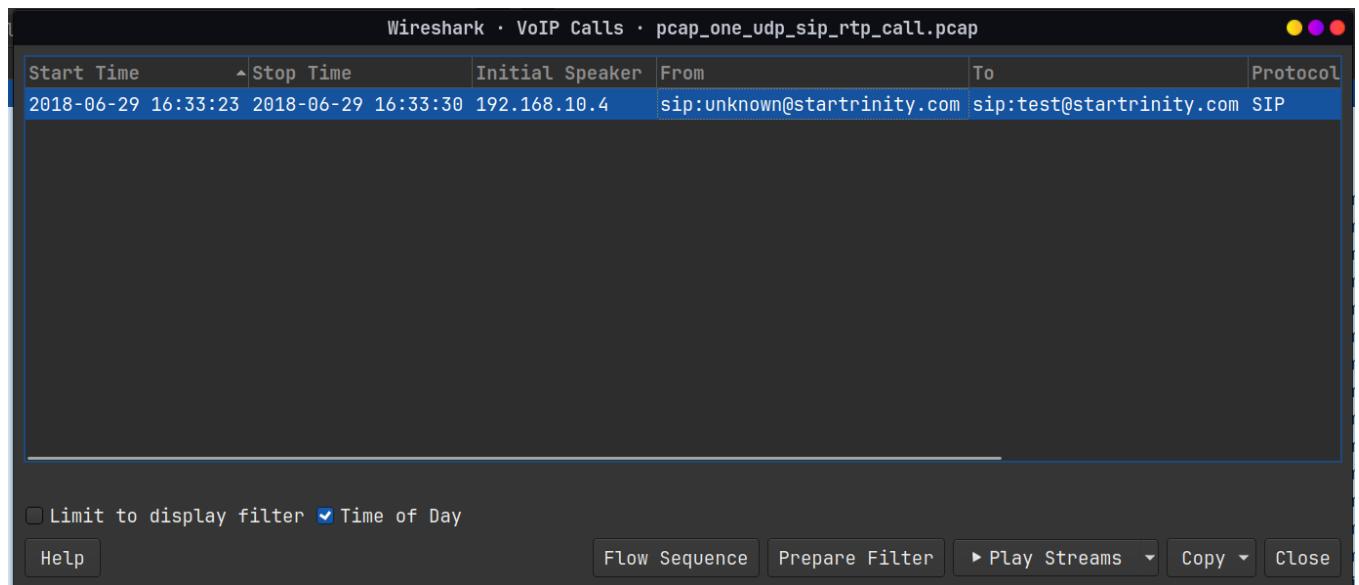
Task2.2: -

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|--------------|--------------|----------|--------|--|
| 1 | 0.000000 | 192.168.10.4 | 5.135.179.50 | SIP/SDP | 940 | Request: INVITE sip:test@startrinity.com |
| 2 | 0.367477 | 5.135.179.50 | 192.168.10.4 | SIP | 399 | Status: 100 Trying |
| 3 | 2.285223 | 5.135.179.50 | 192.168.10.4 | SIP/SDP | 924 | Status: 200 OK (INVITE) |
| 4 | 2.290395 | 192.168.10.4 | 5.135.179.50 | SIP | 412 | Request: ACK sip:test@5.135.179.50:6000 |
| 404 | 6.331187 | 192.168.10.4 | 5.135.179.50 | SIP | 411 | Request: BYE sip:test@5.135.179.50:6000 |
| 410 | 6.416112 | 5.135.179.50 | 192.168.10.4 | SIP | 403 | Status: 200 OK (BYE) |

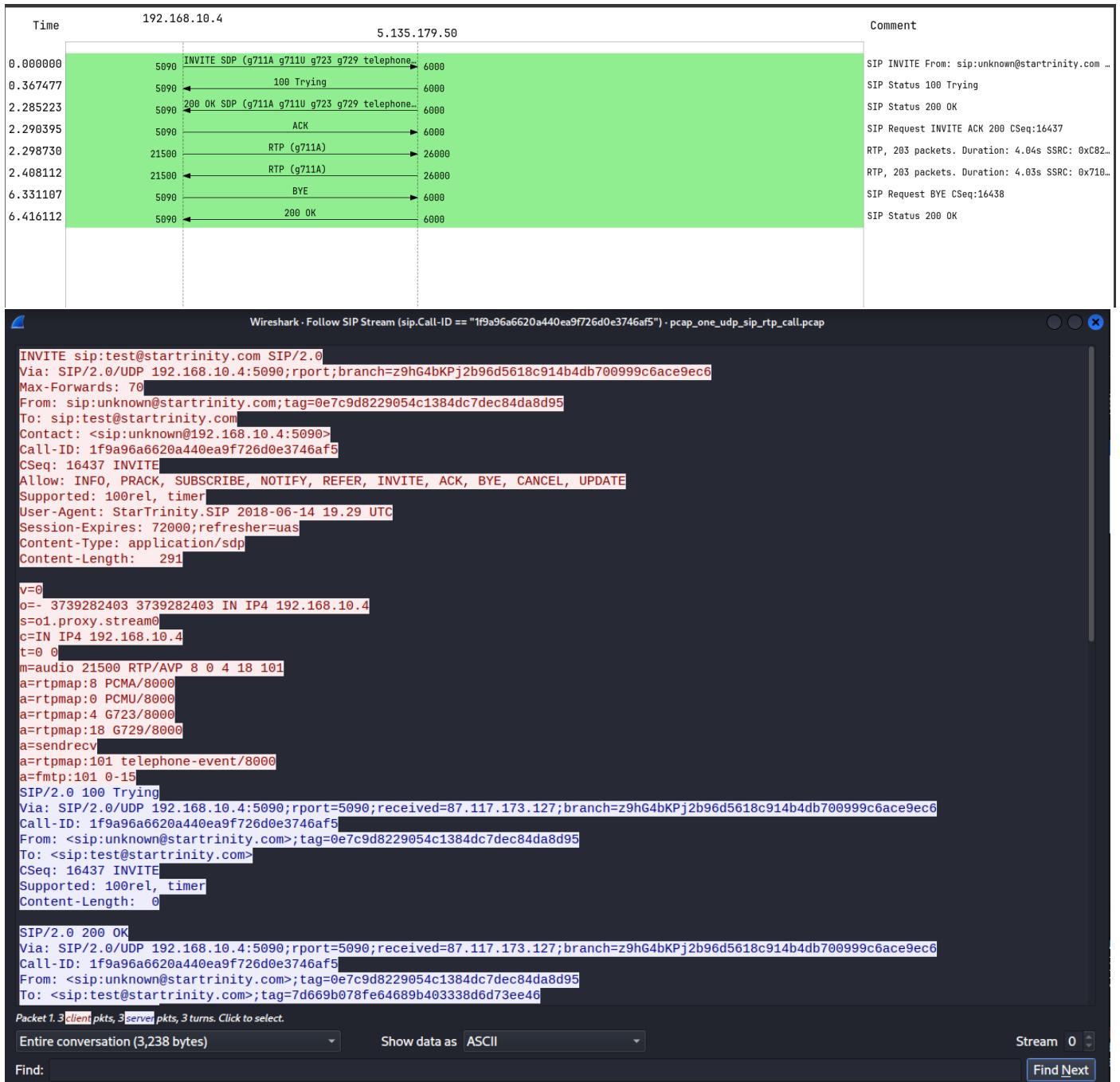
Just 6 SIP endpoints are displayed as we see
at the end of the screenshot Packets: 412
Displayed: 6(1.6%)

406 VoIP calls are displayed as we see at the end of the screenshot Packets: 412 Displayed: 406(98.5%)

Task2.3: -



Task2.4: -



Wireshark - Follow SIP Stream (sip.Call-ID == "1f9a96a6620a440ea9f726d0e3746af5") · pcap_one_udp_sip_rtp_call.pcap

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.10.4:5090; rport=5090; received=87.117.173.127; branch=z9hG4bKPj2b96d5618c914b4db700999c6ace9ec6
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
From: <sip:unknown@startrinity.com>;tag=0e7c9d8229054c1384dc7dec84da8d95
To: <sip:test@startrinity.com>;tag=7d669b078fe64689b403338d6d73ee46
CSeq: 16437 INVITE
Supported: 100rel, timer
Contact: <sip:test@5.135.179.50:6000>
Allow: INFO, PRACK, SUBSCRIBE, NOTIFY, REFER, INVITE, ACK, BYE, CANCEL, UPDATE
Server: [REDACTED]
Session-Expires: 72000;refresher=uas
Content-Type: application/sdp
Content-Length: 291

V=0
o=- 3739271587 3739271587 IN IP4 5.135.179.50
s=ii.proxy.stream0
c=IN IP4 5.135.179.50
t=0 0
m=audio 26000 RTP/AVP 8 0 4 18 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
a=rtpmap:18 G729/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
ACK sip:test@5.135.179.50:6000 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.4:5090; rport; branch=z9hG4bKPj606fbf1ffa574544a49e63fd29a68101
Max-Forwards: 70
From: sip:unknown@startrinity.com;tag=0e7c9d8229054c1384dc7dec84da8d95
To: sip:test@startrinity.com;tag=7d669b078fe64689b403338d6d73ee46
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
CSeq: 16437 ACK
Content-Length: 0

BYE sip:test@5.135.179.50:6000 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.4:5090; rport; branch=z9hG4bKPj487d69b4835c46059705d65707e00950
Max-Forwards: 70
From: sip:unknown@startrinity.com;tag=0e7c9d8229054c1384dc7dec84da8d95
To: sip:test@startrinity.com;tag=7d669b078fe64689b403338d6d73ee46
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
CSeq: 16438 BYE
Content-Length: 0

Packet 3. 3 client pkts, 3 server pkts, 3 turns. Click to select.

```

Entire conversation (3,238 bytes) Show data as ASCII Stream 0

Find: Find Next

```

BYE sip:test@5.135.179.50:6000 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.4:5090; rport; branch=z9hG4bKPj487d69b4835c46059705d65707e00950
Max-Forwards: 70
From: sip:unknown@startrinity.com;tag=0e7c9d8229054c1384dc7dec84da8d95
To: sip:test@startrinity.com;tag=7d669b078fe64689b403338d6d73ee46
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
CSeq: 16438 BYE
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.10.4:5090; rport=5090; received=87.117.173.127; branch=z9hG4bKPj487d69b4835c46059705d65707e00950
Call-ID: 1f9a96a6620a440ea9f726d0e3746af5
From: <sip:unknown@startrinity.com>;tag=0e7c9d8229054c1384dc7dec84da8d95
To: <sip:test@startrinity.com>;tag=7d669b078fe64689b403338d6d73ee46
CSeq: 16438 BYE
Content-Length: 0

```

Scenario 3: Password Cracking using HashCat and John the ripper tools

Task3.1: -

```
(kali㉿kali)-[~/Desktop]
$ curl -L "https://drive.google.com/uc?export=download&id=1BaGW_9c1_KWRzRehcvW_LJj0lYJtV66c" -o simple_hash.txt
% Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
0       0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
100  170  100  170      0      0  124      0  0:00:01  0:00:01 --:--:-- 281

(kali㉿kali)-[~/Desktop]
$ cat simple_hash.txt
203ad5ffa1d7c650ad681fdff3965cd2
bd1d7b0809e4b4ee9ca307aa5308ea6f
e99a18c428cb38d5f260853678922e03
8afab847f50a716e64932d995c8e7435a
3b03c7ea09871a75dce2e403ef2811f

(kali㉿kali)-[~/Desktop]
$
```

```
(kali㉿kali)-[~/Desktop]
$ curl -L "https://drive.google.com/uc?export=download&id=19YtGKwfACX6pibwthMttx25JT_hEuUm6Q" -o complex_hash.txt
% Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total Spent   Left Speed
0       0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
100  168  100  168      0      0  126      0  0:00:01  0:00:01 --:--:-- 257

(kali㉿kali)-[~/Desktop]
$ cat complex_hash.txt
8a24367a1f46c141048752f2d5bbd14b
4ece57a61323b52ccffdbe021956754
78d8707579eab0695d5eaf80b072df14
b2d5d613de0611a5e71110c381dc63dc
7e62797fbcd4b3e787d1364cae3cf263

(kali㉿kali)-[~/Desktop]
$
```

```
(kali㉿kali)-[~/Desktop]
$ hashid < simple_hash.txt
(kali㉿kali)-[~/Desktop]
$ hashid < complex_hash.txt
```

MD5 is the algorithm which is used.

Task3.2: -

The path is

/usr/share/wordlists/rockyou.txt.gz

```
[root@kali]# find / -name rockyou.*  
/usr/share/wordlists/rockyou.txt.gz
```

Simple_hash: -

```
[kali㉿kali]# hashcat -m 0 -a 0 /home/kali/Desktop/simple_hash.txt /usr/share/wordlists/rockyou.txt -o --force  
hashcat (v6.2.6) starting  
You have enabled --force to bypass dangerous warnings and errors!  
This can hide serious problems and should only be done when debugging.  
Do not report hashcat issues encountered when using --force.  
OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEPF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]  
* Device #1: pthread-sandybridge-12th Gen Intel(R) Core(TM) i7-12700H, 2138/4340 MB (1024 MB allocatable), 10MCU  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 31  
INFO: All hashes found as potfile and/or empty entries! Use --show to display them.  
Started: Sun Dec 24 13:36:59 2023  
Stopped: Sun Dec 24 13:36:59 2023  
[kali㉿kali]# hashcat -m 0 -a 0 /home/kali/Desktop/simple_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show  
203ad5ffad7c650ad681fdff3965cd2:Hello1  
bd1d7b0b809e4b4ee9ca307aa5308ea6f:mon  
e99a18c428cb38d5f26085367892e03:abc123  
8af8a47f50a716e64932d995c8e7435a:princess  
3b03c7ea09871a75dce2e403ef2811f:happy1
```

Complex_hash:-

```
[kali㉿kali]# hashcat -m 0 -a 0 /home/kali/Desktop/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force  
hashcat (v6.2.6) starting
```

```
[kali㉿kali]# hashcat -m 0 -a 0 /home/kali/Desktop/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show  
8a24367a1f46c141048752f2d5bbd14b:P@ssw0rd!
```

Just one hash is found.

Task3.3: -

“Simple_hash.txt”: -

203ad5ffa1d7c650ad681fdff3965cd2:hello1
bd1d7b0809e4b4ee9ca307aa5308ea6f:mom
e99a18c428cb38d5f260853678922e03:abc123
8afa847f50a716e64932d995c8e7435a:princess
3b03c7ea09871a75dce2e403ef28111f:happy1

It was so easy and fast to crack simple_hash.txt passwords and I used -a 0 which is “straight”

Attack mode

- 0 = Straight
- 1 = Combination
- 3 = Brute-force
- 6 = Hybrid Wordlist + Mask
- 7 = Hybrid Mask + Wordlist

“complex_hash.txt”: -

8a24367a1f46c141048752f2d5bbd14b:P@ssw0rd!

And the other hashes were not found.

It was not as fast as simple hash

And other hashes is not crackable.

Outcome of simple_hash.txt: -

```
(kali㉿kali)-[~/Desktop]
$ hashcat -m 0 -a 0 /home/kali/Desktop/simple_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show
203ad5ff1d7c650ad681fdff3965cd2:hello1
bd1d7b0b809e4b4ee9ca307aa5308ea6f:mom
e99a18c428cb38d5f260853678922e03:abc123
8afab47ff50a716e64932d995c8e7435a:princess
3b03c7ea09871a75dce2e403ef2811f:happy1
```

Outcome of complex_hash.txt: -

```
(kali㉿kali)-[~/Desktop]
$ hashcat -m 0 -a 0 /home/kali/Desktop/complex_hash.txt /usr/share/wordlists/rockyou.txt -o --force --show
8a24367a1f46c141048752f2d5bbd14b:P@ssw0rd!
```

Task3.4: -

```
(kali㉿kali)-[~/Desktop]
$ curl -L "https://drive.google.com/uc?export=download&id=1uHHxXyPzwsUlWKLBr0jpwHKiyM1N3" -o hash1.txt
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total Spent   Left Speed
0       0      0      0      0      0  --:--:--:--:--:--:--:--:--:--:--:0
100  168  100  168      0      0  126      0  0:00:01  0:00:01  --:--:-- 164k

(kali㉿kali)-[~/Desktop]
$ cat hash1.txt
3c086ff596b4ae58e1d71b3626fefc87
4913a9178621eadcdf191db17915fbcb
608f0b988db4a96066af7dd8870de96c
6e0b7076126a295dfcd54835387b7b
d2feb9b6718bb374dfdd689380676954
```

```
(kali㉿kali)-[~/Desktop]
└─$ curl -L "https://drive.google.com/uc?export=download&id=1JLBAAuUd3wcbzAs6JRnxNYitKFmLWRTqu" -o hash2.txt
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total Spent   Left Speed
0       0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0
100  208 100  208      0      0  152      0  0:00:01  0:00:01 --:--:-- 562

(kali㉿kali)-[~/Desktop]
└─$ cat hash2.txt
59c826fc854197cbd4d1083bce8fc00d0761e8b3
7288edd0fc3ffcb93a0cf06e3568e28521687bc
5a46b8253d07320a14cace9b4dcfb80f93dcef04
5049c40354abbd47f246f9204467548e39df6f8
23d42f5f3f66498b2c8ff4c20b8c5ac826e47146
```

MD5 is the algorithm which is used in hash1.

```
$ hashid < hash1.txt
```

SHA-1 is the algorithm which is used in hash 2

```
(kali㉿kali)-[~/Desktop]
└─$ hashid < hash2.txt
```

Task3.5: -

Hash1.txt: -

```
(kali㉿kali)-[~/Desktop]
└─$ john hash1.txt --format=RAW-MD5
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=10
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
alb2c3      (?)
flower      (?)
unix        (?)
Proceeding with incremental:ASCII
john123      (?)
rockstar    (?)
5g 0:00:01:01 DONE 3/3 (2023-12-24 14:34) 0.08110g/s 55177Kp/s 55177Kc/s 55200KC/s rockpon..rockstay
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Desktop]
└─$ john hash1.txt --format=RAW-MD5 --show
?:alb2c3
?:unix
?:flower
?:john123
?:rockstar

5 password hashes cracked, 0 left
```

Hash2.txt: -

```
(kali㉿kali)-[~/Desktop]
└─$ john hash2.txt --format=RAW-SHA1
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=10
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
```

```
(kali㉿kali)-[~/Desktop]
└─$ john hash2.txt --format=RAW-SHA1 --show
?:cookie
?:test123
?:flower

3 password hashes cracked, 2 left
```

Task3.6: -

Hash1.txt: -

3c086f596b4aee58e1d71b3626fefc87:a1b2c3

4913a9178621eadcdf191db17915fbcb:unix

608f0b988db4a96066af7dd8870de96c:flower

6e0b7076126a29d5dfcbd54835387b7b:john123

d2feb9b6718bb374dfdd689380676954:rockstar

```
(kali㉿kali)-[~/Desktop]
└─$ john hash1.txt --format=RAW-MD5 --show
?:a1b2c3
?:unix
?:flower
?:john123
?:rockstar

5 password hashes cracked, 0 left
```

Hash2.txt: -

59c826fc854197cbd4d1083bce8fc00d0761e8b3:cookie

7288edd0fc3ffcbef93a0cf06e3568e28521687bc:test123

5a46b8253d07320a14cace9b4dcbf80f93dcef04:flower

5049c40354ababd47f246f9204467548e39df6f8: NOT FOUND

23d42f5f3f66498b2c8ff4c20b8c5ac826e47146: NOT FOUND

```
(kali㉿kali)-[~/Desktop]
$ john hash2.txt --format=RAW-SHA1 --show
?:cookie
?:test123
?:flower

3 password hashes cracked, 2 left
```

The passwords were easy to crack since they were popular words and sequences.

The last 2 hashes in hash2.txt couldn't be cracked using john the ripper

Scenario 4: Manual SQL injection

Task4.1: -

The screenshot shows a web application interface for 'Altoro Mutual'. At the top, there's a navigation bar with links for 'Sign Off', 'Contact Us', 'Feedback', 'Search', and a 'Go' button. To the right of the search bar is a green button labeled 'DEMO SITE ONLY'. Below the navigation, there are tabs for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is selected. On the left, there's a sidebar with sections for 'I WANT TO ...' (View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, Customize Site Language) and 'ADMINISTRATION' (Edit Users). The main content area displays a message: 'Hello Admin User' followed by 'Welcome to Altoro Mutual Online.' A dropdown menu shows 'View Account Details: 800000 Corporate' with a 'GO' button. Below this, a 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click Here to apply.' At the bottom of the page, there's a footer with links for 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information: 'Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd.. All rights reserved.' There's also a note: 'The Altoro3 website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/zeoscan/>'.

Task4.2: -

| Transaction ID | Transaction Time | Account ID | Action | Amount |
|----------------|------------------|------------|------------|------------|
| 12832 | 2023-12-24 13:48 | 800001 | Deposit | \$1000.00 |
| 12831 | 2023-12-24 13:48 | 800000 | Withdrawal | -\$1000.00 |

Task4.3: -

1. The website is vulnerable to SQL injection
 - a- Injection can have severe impacts on a system. An attacker may manipulate input to execute unauthorized SQL commands, leading to data exposure, modification, or even deletion
 - b- Parameterized queries, and prepared statements can help mitigate SQL injection risks.

2. Username: ahmed' or 1=1--

Password: anypasswordcanwork

```
SELECT * FROM users WHERE  
username='ahmed' or 1=1-- 'and  
password='any password can word'.
```

-- character ignores the part after its position.
So the query only checks the username and
the attacker will gain access to the admin
account.

| | |
|--------------------------------------|--|
| Username: | <input type="text" value="ahmed' or 1=1--"/> |
| Password: | <input type="password" value="*****"/> |
| <input type="button" value="Login"/> | |

3.

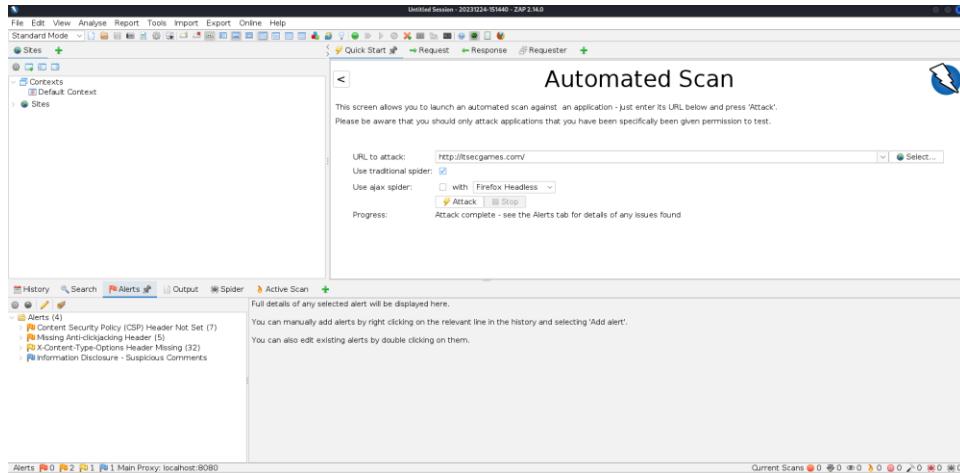


Scenario 5: Running pen-tests on a website using ZAP

Task5.1: -

1. Active scanning in Zed Attack Proxy (ZAP) involves using a traditional spider to crawl through a target application. After configuring ZAP and the browser proxy settings, the spider is launched to explore the application's structure. Once the spidering is complete, automated scanning is initiated, actively probing for vulnerabilities based on the identified structure. The results are then reviewed, categorizing vulnerabilities by severity.

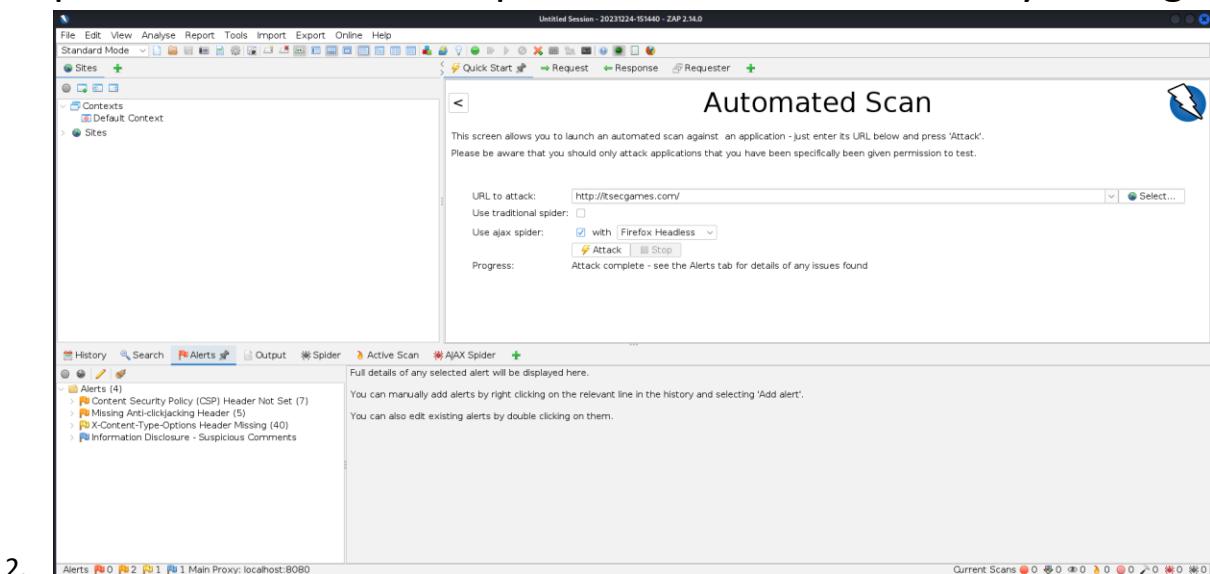
ZAP allows for the generation of detailed reports, aiding in the analysis and remediation of security issues. It is crucial to perform such scans with proper authorization and adhere to ethical hacking guidelines to ensure responsible and legal practices.



Task5.2: -

1. To perform automated scanning with the Ajax Spider in Zed Attack Proxy (ZAP), begin by configuring ZAP and setting up the browser to proxy through it. In the Ajax Spider tab, specify the target URL and initiate the dynamic crawling process, allowing the tool to handle asynchronous requests and discover dynamic content, including JavaScript-driven interactions. Once the spidering is complete, move to the Automated Scan tab, configure the scan settings, and commence the automated scanning process. ZAP will actively send requests, leveraging insights from the Ajax Spider, to identify and assess vulnerabilities in the target application. Review the comprehensive scan results and generate detailed reports using ZAP. It is essential to conduct these scans with

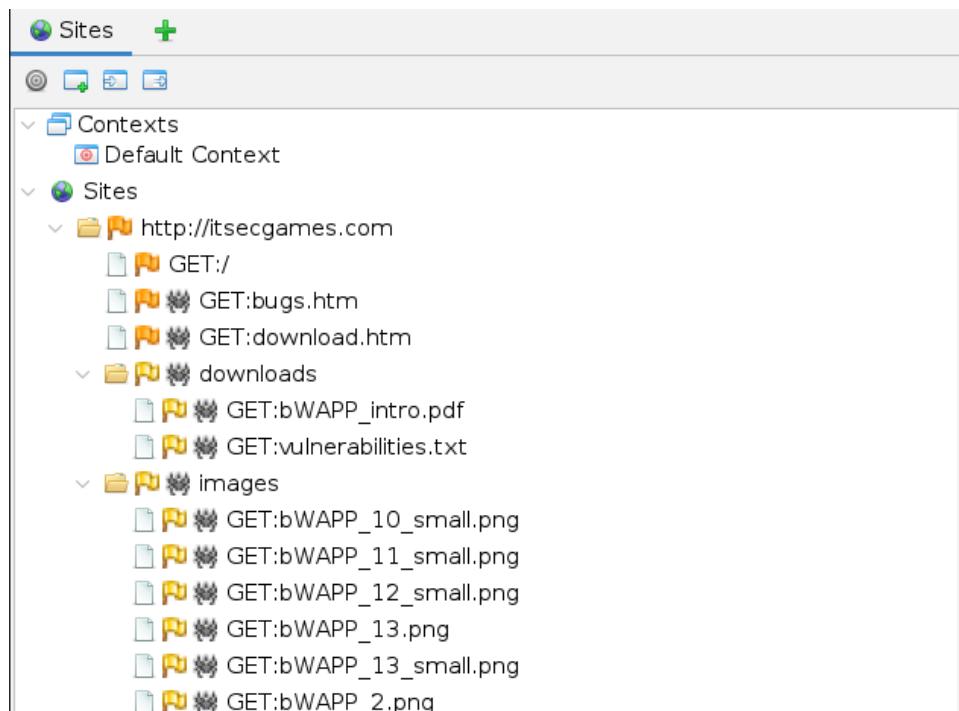
proper authorization and adhere to ethical hacking practices to ensure responsible and lawful security testing.



2.

Task5.3: -

1. Traditional spider tree



File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

GET:bWAPP_2_small.png
GET:bWAPP_3.png
GET:bWAPP_3_small.png
GET:bWAPP_4.png
GET:bWAPP_4_small.png
GET:bWAPP_5.png
GET:bWAPP_5_small.png
GET:bWAPP_6.png
GET:bWAPP_6_small.png
GET:bWAPP_7.png
GET:bWAPP_7_small.png
GET:bWAPP_8.png
GET:bWAPP_8_small.png
GET:bWAPP_9.png
GET:bWAPP_9_small.png
GET:bee_1.png
GET:favicon.ico

Sites +

GET:bWAPP_6_small.png
GET:bWAPP_7.png
GET:bWAPP_7_small.png
GET:bWAPP_8.png
GET:bWAPP_8_small.png
GET:bWAPP_9.png
GET:bWAPP_9_small.png
GET:bee_1.png
GET:favicon.ico
GET:index.htm
js
GET:html5.js
GET:robots.txt
GET:sitemap.xml
stylesheets
GET:stylesheet.css
GET:training.htm

2. Ajax spider tree



Sites +

GET:bWAPP_2.png
GET:bWAPP_2_small.png
GET:bWAPP_3.png
GET:bWAPP_3_small.png
GET:bWAPP_4_small.png
GET:bWAPP_5_small.png
GET:bWAPP_6_small.png
GET:bWAPP_7_small.png
GET:bWAPP_8.png
GET:bWAPP_8_small.png
GET:bWAPP_9.png
GET:bWAPP_9_small.png
GET:bee_1.png
GET:bg_1.jpg
GET:bg_3.jpg
GET:blogger.png
GET:cc.png

Sites +

GET:bg_3.jpg
GET:blogger.png
GET:cc.png
GET:facebook.png
GET:favicon.ico
GET:linkedin.png
GET:mme.png
GET:owasp.png
GET:twitter.png
GET:index.htm
js
GET:html5.js
GET:robots.txt
GET:sitemap.xml
stylesheets
GET:stylesheet.css
GET:training.htm

